ние и протоколы обмена данными, при использовании которых риск утечки либо утери информации будет минимален. При наличии некого упрощенного шаблона безопасной информационной среды будет существенно упрощен процесс внедрения концепции в реальные системы.

УДК 004.056 + 519.87

В. В. Царенко
Научный руководитель: доц. В. Ю. Бердюгин
Южно-Уральский государственный университет, Челябинск

МЕТОДОЛОГИЯ МОДЕЛИРОВАНИЯ И ОЦЕНКИ УГРОЗ ФИЗИЧЕСКОГО ДОСТУПА К ОБЪЕКТУ ЗАЩИТЫ

Аннотация. Для информационных систем, изолированных от глобальной сети, одними из наиболее актуальных угроз информационной безопасности и защиты информации являются угрозы физического доступа к элементам данных систем. Таким образом, возникает потребность в объективной оценке вероятности реализации этих угроз. В данной публикации рассмотрена возможность обращения к прикладным методам, составляющим инструментарий математического моделирования, посредством которых возможно представление объекта защиты и поиск путей реализации угроз физического доступа.

Ключевые слова: угрозы физического доступа; инженерно-техническая защита информации; система безопасности; охрана объектов; формализованное представление; безопасность; математическое моделирование; математические модели; математические методы; теория вероятностей; теория графов.

Ввиду разнообразия и уникальности каждого объекта информатизации и в общем случае каждого информационного ресурса, проектирование системы защиты является сложным процессом, в котором преимущественно применяются экспертные знания, опыт специалистов в области систем инженерно-технической защиты информации. Необходимым условием обеспечения комплексной защиты информации является создание определенных критериев, позволяющих оценить защищенность и определить достаточность мер, предпринятых для защиты от угроз. Моделирование позволяет унифицировать систему защиты и установить критерии оценки (показатели) защищенности объекта. Непосредственный интерес представляют математические модели, позволяющие на основании выбранных критериев оценить систему защиты объекта на соответствие предъявляемым требованиям, в частности, оценить

физическую защищенность объекта как элемента инженерно-технической защиты информации.

Для создания достаточно близкой к реальной модели угрозы физического проникновения необходимо проиграть с позиции злоумышленника варианты проникновения к источнику информации. Чем больше при этом будет учтено факторов, влияющих на эффективность проникновения, тем выше адекватность модели. В условии отсутствия информации о злоумышленнике, его квалификации, технической оснащенности, во избежание грубых ошибок лучше переоценить угрозу, чем ее недооценить.

На основе такого подхода модель злоумышленника выглядит следующим образом:

- злоумышленник представляет серьезного противника, тщательно готовящего операцию проникновения, он изучает обстановку вокруг территории организации, наблюдаемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) освещения, а также сотрудников с целью добывания от них информации о способах и средствах защиты;
- имеет в распоряжении современные технические средства проникновения и преодоления механических преград;
- всеми доступными способами добывает и анализирует информацию о расположении зданий и помещений организации, о рубежах охраны, о местах хранения источников информации, видах и типах средств охраны, телевизионного наблюдения, освещения и местах их установки;
- проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи.

При моделировании действий квалифицированного злоумышленника необходимо также исходить из предположения, что он хорошо представляет современное состояние технических средств защиты информации, типовые варианты их применения, слабые места и «мертвые» зоны диаграмм направленности активных средств охраны.

Для оценки физической защищенности объекта необходима модель, которая описывает структуру самого объекта (состав и связи элементов) и содержит описание его составляющих в пространстве. Данные составляющие модели не являются автономными, а взаимно дополняют друг друга.

Оценка показателей угроз безопасности представляет достаточно сложную задачу в силу следующих обстоятельств:

- добывание информации нелегальными путями не афишируется и фактически отсутствуют или очень скудно представлены в литературе реальные статистические данные;

– многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняют возможность выявления и оценки угроз безопасности информации;
– априори не известен состав и характеристики технических средств добывания информации злоумышленника.

Оценки угроз информации в результате проникновения злоумышленника к источнику носят вероятностный характер. При этом рассматривается вероятность реализуемости рассматриваемого пути, а также значимость соответствующего элемента информации.

Более удобным вариантом является представление моделей на основе баз данных, математическое обеспечение которых позволяет учесть связи между элементами объекта, быстро корректировать данные в них и систематизировать элементы по различным признакам, например, по виду, положению в пространстве, способам и средствам защиты, угрозам.

В рамках поставленной задачи выбор методов теории графов в совокупности с методами теории вероятностей представляется наиболее эффективным. Обусловлено данное предложение следующими аспектами:

1) в виде графа возможно представление структуры объекта защиты в необходимой степени (элементы объекта защиты и их местоположение, рубежи защиты, возможность перехода из одной точки объекта в другую);

2) использование методов кратчайшего пути в графе позволяет выявить как наиболее уязвимые элементы объекта защиты, так и потенциальные маршруты доступа к ним со стороны нарушителя, позволяющие ему с высокой вероятностью получить доступ к необходимому ресурсу.

Объект защиты для решения поставленной задачи задается взвешенным ориентированным графом $G = (V, E)$ с весовой функцией w: $E \to \mathbb{R}$, отображающей ребра на их веса, значения которых выражаются действительными числами. Вес пути $p = \langle v_0, v_1, ..., v_k \rangle$ равен суммарному весу входящих в него ребер:

$$w(p) = \sum_{i=1}^{k} w(v_{i-1}, v_i).$$

Вес кратчайшего пути $\delta(u, v)$ из вершины u в вершину v определяется соотношением

$$\delta(u,v) = \begin{cases} \min\{w(p) : u \rightsquigarrow v\}, & \text{если существует путь из } u \text{ в } v, \\ \infty & \text{в противном случае.} \end{cases}$$

Тогда по определению кратчайший путь из вершины в вершину — это любой путь, вес которого удовлетворяет соотношению $w(p) = \delta(u, v)$.

В общем случае, для поиска уязвимых мест объекта защиты, а также потенциальных путей нарушителя обратимся к задаче о кратчайшем пути между всеми вершинами. В данной задаче требуется найти кратчайший путь из каждой вершины в каждую вершину.

Далее обратимся к представлению графа, необходимому для применения соответствующей группы алгоритмов.

Имеется два стандартных способа представления графа $G = (V, E)$: как набора списков смежных вершин и как матрицы смежности. Оба способа представления применимы как для ориентированных, так и для неориентированных графов.

Остановимся на представлении графа в виде матрицы смежности. Для удобства предполагается, что вершины пронумерованы как 1, 2, …, n. В нашем случае представление графа G с использованием матрицы смежности представляет собой матрицу W размером $n \times n$, содержащей веса ориентированных ребер (дуг) ориентированного графа $G = (V, E)$ с n вершинами:

$$w_{ij} = \begin{cases} 0, & \text{если } i = j, \\ w(i, j), & \text{если } i \neq j \text{ и } (i, j) \in E, \\ \infty, & \text{если } i \neq j \text{ и } (i, j) \notin E. \end{cases}$$

Отметим, что наличие ребер с отрицательным весом допускается. Возможность работы с ними зависит от выбранного алгоритма поиска кратчайшего пути, его модификации.

В оценке физической защищенности, поиск уязвимых мест объекта защиты, а также маршрутов реализации угроз физического доступа, объективная составляющая обеспечивается использованием математических моделей и алгоритмов работы с ними. Субъективная составляющая привносится непосредственно на этапе формализации объекта защиты, что определяет качество исходного результата.

Оценка физической защищенности носит комплексный характер. Она учитывает оценку условий, в которых приходится решать поставленную задачу, оценки вероятного противника и объекта защиты.